M. Frączyk *et al.* (2020) "Counting Bounded Elements of a Number Field,"
International Mathematics Research Notices, Vol. 00, No. 0, pp. 1–18
doi:10.1093/imrn/rnaa126

Counting Bounded Elements of a Number Field

Mikołaj Fraczyk[1,2,4], Gergely Harcos[1,3,5] and Péter Maga[1,3,*]

[1]Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, POB 127, Budapest H-1364, Hungary, [2]MTA Rényi Intézet Lendület Groups and Graphs Research Group, [3]MTA Rényi Intézet Lendület Automorphic Research Group, [4]Institute for Advanced Study, Princeton, NJ, USA, and [5]Central European University, Nador u. 9, Budapest H-1051, Hungary

[*]*Correspondence to be sent to: e-mail: magapeter@gmail.com*

We estimate, in a number field, the number of elements and the maximal number of linearly independent elements, with prescribed bounds on their valuations. As a by-product, we obtain new bounds for the successive minima of ideal lattices. Our arguments combine group theory, ramification theory, and the geometry of numbers.

1 Introduction

It was a decisive moment in the history of mathematics when Minkowski [12] realized that certain geometric ideas are very powerful in tackling difficult arithmetic problems. In particular, Minkowski [12] proved that in a number field k of degree $d > 1$ and discriminant Δ, every ideal class can be represented by an integral ideal of norm less than $|\Delta|^{1/2}$. His proof relied on two ideas. First, the natural embedding $k \hookrightarrow k \otimes_{\mathbb{Q}} \mathbb{R}$ allows one to regard the ring of integers $\mathfrak{o}$ as a lattice in $\mathbb{R}^d$ of covolume $|\Delta|^{1/2}$. Second, a lattice in $\mathbb{R}^d$ contains a nonzero lattice point in a convex body symmetric about the origin, as long as the volume of the body exceeds 2^d times the covolume of the lattice. Here and later, a convex body means a convex, compact set with non-empty interior in the ambient Euclidean space. The second idea was extended by Blichfeldt [2] and

Received November 19, 2019; Revised April 8, 2020; Accepted May 7, 2020
Communicated by Prof. Valentin Blomer

van der Corput [4] to exhibit more lattice points in larger convex bodies. It leads to the following estimate that we state partly for motivation, partly as a technical ingredient for our investigations. For a modern exposition of the quoted results, see [6, Chapter 2, Sections 5.1 and 7.2].

Theorem 1 (Minkowski [12], Blichfeldt [2], van der Corput [4]). Let $\mathfrak{n} \subset \mathfrak{o}$ be a nonzero ideal, and let $\mathcal{B} \subset k \otimes_{\mathbb{Q}} \mathbb{R}$ be a convex body symmetric about the origin. Then,

$$|\mathfrak{n} \cap \mathcal{B}| \geqslant \frac{\operatorname{vol}(\mathcal{B})}{2^d |\Delta|^{1/2} [\mathfrak{o} : \mathfrak{n}]}.$$

Blichfeldt [2] also established an upper bound of similar quality in the case when $\mathfrak{n} \cap \mathcal{B}$ contains d linearly independent vectors.

Theorem 2 (Blichfeldt [2]). Let $\mathfrak{n} \subset \mathfrak{o}$ be a nonzero ideal, and let $\mathcal{B} \subset k \otimes_{\mathbb{Q}} \mathbb{R}$ be a convex body symmetric about the origin. Assume that $\mathfrak{n} \cap \mathcal{B}$ contains d linearly independent vectors. Then,

$$|\mathfrak{n} \cap \mathcal{B}| \leqslant \frac{(d+1)! \operatorname{vol}(\mathcal{B})}{|\Delta|^{1/2} [\mathfrak{o} : \mathfrak{n}]}.$$

In fact, Blichfeldt proved a more general result, namely Theorem 7 in Section 3. The original source [2] is an account of an AMS Sectional Meeting held in 1920 (written by B. A. Bernstein), so it does not contain any proof. What is worse, we could only find sketches of the proof in the literature. Hence, we include a detailed proof in Section 3, without claiming any originality.

Our principal goal in this paper is to provide an upper bound for $|\mathfrak{n} \cap \mathcal{B}|$ in the complementary case when $\mathfrak{n} \cap \mathcal{B}$ does not contain d linearly independent vectors. More precisely, with certain arithmetic applications in mind, we restrict ourselves to the special convex bodies considered by Minkowski [12] in his seminal work. They are the archimedean analogues of ideal lattices, and they are defined as follows. As before, let k be a number field of degree $d > 1$. Let $\Sigma := \operatorname{Hom}(k, \overline{\mathbb{Q}})$, and let K be the compositum of the fields $\sigma(k)$ for $\sigma \in \Sigma$. Then, $K/\mathbb{Q}$ is a finite Galois extension whose Galois group $G := \operatorname{Gal}(K/\mathbb{Q})$ acts transitively and faithfully on Σ. In this way, G is a transitive permutation group of degree d. Fixing an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, we can think of the elements of Σ as the embeddings $\sigma : k \hookrightarrow \mathbb{C}$, and we can identify $k \otimes_{\mathbb{Q}} \mathbb{R}$ with the set of column vectors $(z_\sigma) \in \mathbb{C}^\Sigma$ satisfying $z_{\overline{\sigma}} = \overline{z_\sigma}$ for all $\sigma \in \Sigma$. See [13, Chapter I, Section 5] for more details. Let (B_σ) be a collection of positive numbers such that $B_{\overline{\sigma}} = B_\sigma$ for all

$\sigma \in \Sigma$. We shall focus on convex bodies of the form

$$\mathcal{B} := \left\{(z_\sigma) \in \mathbb{C}^\Sigma : z_{\overline{\sigma}} = \overline{z_\sigma} \text{ and } |z_\sigma| \leqslant B_\sigma \text{ for all } \sigma \in \Sigma\right\}, \tag{1}$$

and we note for later reference that

$$\mathrm{vol}(\mathcal{B}) \asymp_d \prod_{\sigma \in \Sigma} B_\sigma. \tag{2}$$

Here and later, the symbols $\ll_d$, $\gg_d$, $\asymp_d$ have their usual meaning in analytic number theory: $X \ll_d Y$ (resp. $Y \gg_d X$) means that $|X| \leqslant CY$ holds for an absolute constant $C > 0$ depending only on d, while $X \asymp_d Y$ abbreviates $X \ll_d Y \ll_d X$.

Theorem 3. Let $\mathfrak{n} \subset \mathfrak{o}$ be a nonzero ideal, and let $\mathcal{B} \subset k \otimes_{\mathbb{Q}} \mathbb{R}$ be a convex body of the form (1). Let m be the maximal number of linearly independent lattice vectors contained in $\mathfrak{n} \cap \mathcal{B}$. If $m < d$, then

$$|\mathfrak{n} \cap \mathcal{B}| \ll_d |\Delta|^{\min\left(\frac{1}{2}, \frac{m}{2d-2m}\right)}. \tag{3}$$

Further, if $m < d$ and G is 2-homogeneous (i.e., it acts transitively on the 2-element subsets of Σ), then

$$|\mathfrak{n} \cap \mathcal{B}| \ll_d |\Delta|^{\frac{m}{2d-2}}. \tag{4}$$

Theorems 2 and 3 yield a practical estimate for the number of elements of k that are bounded in every archimedean and non-archimedean valuation of k.

Corollary 1. Let $\mathfrak{n} \subset \mathfrak{o}$ be a nonzero ideal, and let $\mathcal{B} \subset k \otimes_{\mathbb{Q}} \mathbb{R}$ be a convex body of the form (1). Then,

$$|\mathfrak{n} \cap \mathcal{B}| \ll_d |\Delta|^{1/2} + \frac{\mathrm{vol}(\mathcal{B})}{|\Delta|^{1/2}[\mathfrak{o} : \mathfrak{n}]}. \tag{5}$$

By combining Theorems 1 and 3, we see that if the volume of our convex body is sufficiently large compared with the covolume of our ideal lattice, then the intersection contains several linearly independent lattice vectors.

Corollary 2. Let $\mathfrak{n} \subset \mathfrak{o}$ be a nonzero ideal, and let $\mathcal{B} \subset k \otimes_{\mathbb{Q}} \mathbb{R}$ be a convex body of the form (1). Let m be the maximal number of linearly independent lattice vectors contained in $\mathfrak{n} \cap \mathcal{B}$. If $m < d$, then

$$\mathrm{vol}(\mathcal{B}) \ll_d |\Delta|^{\min\left(1, \frac{d}{2d-2m}\right)}[\mathfrak{o} : \mathfrak{n}]. \tag{6}$$

Further, if $m < d$ and G is 2-homogeneous, then

$$\mathrm{vol}(\mathcal{B}) \ll_d |\Delta|^{\frac{d-1+m}{2d-2}}[\mathfrak{o} : \mathfrak{n}]. \tag{7}$$

If $m = 0$, then (3) and (4) are trivial, while (6) and (7) boil down to the Minkowski bound $\mathrm{vol}(\mathcal{B}) \ll_d |\Delta|^{1/2}[\mathfrak{o} : \mathfrak{n}]$. If $m = 1$ or $m = d - 1$, then (3) and (4) (resp. (6) and (7)) are identical. For $2 \leqslant m \leqslant d - 2$, the bound (4) is stronger than (3) (resp. (7) is stronger than (6)), but its scope is restricted by the assumption that G is 2-homogeneous. The list of finite 2-homogeneous groups is known by the work of many people, in particular by the classification of finite simple groups. For further details and references, see [8, Proposition 3.1], [3, Theorem 5.3], [7, p. 198]. We emphasize that Corollaries 1 and 2 are arithmetic in nature, that is, they would break down for general lattices in $k \otimes_{\mathbb{Q}} \mathbb{R}$.

Corollary 3. Let $\mathfrak{n} \subset \mathfrak{o}$ be a nonzero ideal, and let $\mathcal{B} \subset k \otimes_{\mathbb{Q}} \mathbb{R}$ be a convex body of the form (1). If $\mathcal{B}$ does not contain a lattice basis of $\mathfrak{n}$, then $\mathrm{vol}(\mathcal{B}) \ll_d |\Delta|[\mathfrak{o} : \mathfrak{n}]$.

Interestingly, when k is totally real, the conclusion of Corollary 3 also follows from a celebrated result of McMullen [11, Theorem 4.1] proved by topological arguments. In another direction, when the radii B_σ are equal, the conclusion of Corollary 3 says that the last successive minimum of $\mathfrak{n}$ is $\ll_d |\Delta|^{1/d}[\mathfrak{o} : \mathfrak{n}]^{1/d}$. Here and later, we understand successive minima with respect to the closed Euclidean ball centered at the origin. For $\mathfrak{n} = \mathfrak{o}$, this bound was deduced earlier by Bhargava *et al.* [1, Theorem 1.6] with a more direct approach. We will return to these connections in Section 4. In fact, we can control, to some extent, all successive minima of ideal lattices.

Theorem 4. Let $\lambda_1 \leqslant \cdots \leqslant \lambda_d$ be the successive minima of a nonzero ideal $\mathfrak{n} \subset \mathfrak{o}$ embedded as a lattice in $k \otimes_{\mathbb{Q}} \mathbb{R}$. Then, for all $m \in \{1, \ldots, d - 1\}$, we have

$$\lambda_1 \cdots \lambda_m \gg_d |\Delta|^{\max\left(0, \frac{m}{d} - \frac{1}{2}\right)}[\mathfrak{o} : \mathfrak{n}]^{\frac{m}{d}}; \tag{8}$$

$$\lambda_{m+1}\lambda_{m+2} \cdots \lambda_d \ll_d |\Delta|^{\min\left(\frac{1}{2}, 1 - \frac{m}{d}\right)}[\mathfrak{o} : \mathfrak{n}]^{1 - \frac{m}{d}}. \tag{9}$$

If G is 2-homogeneous, then the exponents of $|\Delta|$ in (8) and (9) can be improved to $\frac{m(m-1)}{2d(d-1)}$ and $\frac{(d-m)(d+m-1)}{2d(d-1)}$, respectively.

The example $k = \mathbb{Q}(p^{1/d})$ mentioned by Bhargava *et al.* below their [1, Theorem 1.6] shows that the 2-homogeneous case of Theorem 4 cannot be improved in general. Indeed, if $p > d > 1$ are prime numbers and $\mathfrak{n} = \mathfrak{o}$, then $G \cong \mathrm{Aff}(\mathbb{F}_d) \cong (\mathbb{Z}/d\mathbb{Z}) \rtimes$

$(\mathbb{Z}/d\mathbb{Z})^\times$ is sharply 2-transitive, while $\lambda_m \asymp_d |\Delta|^{\frac{m-1}{d(d-1)}}$ holds for all $m \in \{1,\dots,d\}$. The last relation follows from the straightforward upper bound $\lambda_m \ll_d p^{\frac{m-1}{d}}$ combined with $|\Delta| \asymp_d p^{d-1}$ and Minkowski's result (12) quoted below. The same example also shows that Corollary 3 cannot be improved in general. In contrast, the sharpness of (3)–(4) and (8)–(9) is less clear to us.

Theorem 4 readily yields two-sided bounds for individual successive minima, extending the result of Bhargava *et al.* [1, Theorem 1.6] mentioned in the previous paragraph.

Corollary 4. Let $\lambda_1 \leqslant \cdots \leqslant \lambda_d$ be the successive minima of a nonzero ideal $\mathfrak{n} \subset \mathfrak{o}$ embedded as a lattice in $k \otimes_{\mathbb{Q}} \mathbb{R}$. Then, for all $m \in \{1,\dots,d\}$, we have

$$\Delta^{\max\left(0,\frac{1}{d}-\frac{1}{2m}\right)}[\mathfrak{o}:\mathfrak{n}]^{\frac{1}{d}} \ll_d \lambda_m \ll_d \Delta^{\min\left(\frac{1}{2d-2m+2},\frac{1}{d}\right)}[\mathfrak{o}:\mathfrak{n}]^{\frac{1}{d}} \qquad \text{in general;} \tag{10}$$

$$\Delta^{\frac{m-1}{2d(d-1)}}[\mathfrak{o}:\mathfrak{n}]^{\frac{1}{d}} \ll_d \lambda_m \ll_d \Delta^{\frac{d+m-2}{2d(d-1)}}[\mathfrak{o}:\mathfrak{n}]^{\frac{1}{d}} \qquad \text{if } G \text{ is 2-homogeneous.} \tag{11}$$

To form an idea of the accuracy of (11), it is instructive to observe that the two sides differ by a factor of $\Delta^{\frac{1}{2d}}$. Moreover, the product of the left-hand side over $m \in \{1,\dots,d\}$ equals $\Delta^{\frac{1}{4}}[\mathfrak{o}:\mathfrak{n}]$, while the same for the right-hand side equals $\Delta^{\frac{3}{4}}[\mathfrak{o}:\mathfrak{n}]$. This should be compared with the product of the λ_ms, which by Minkowski's theorem [6, p. 124, Theorem 3] is

$$\lambda_1 \cdots \lambda_d \asymp_d |\Delta|^{\frac{1}{2}}[\mathfrak{o}:\mathfrak{n}]. \tag{12}$$

The proof of Theorem 3 combines group theory, ramification theory, and the geometry of numbers. The main idea is to obtain an upper bound for $|\mathfrak{n}\cap\mathcal{B}|$ by projecting $\mathfrak{n}\cap\mathcal{B}$ onto well-chosen "coordinate subspaces" $\mathbb{R}^S$ of $\mathbb{C}^\Sigma$ for $S \subset \Sigma$, and then compare it with the lower bound of Theorem 1. We make sure that the projections of $\mathfrak{n}\cap\mathcal{B}$ generate lattices in their ambient spaces $\mathbb{R}^S$, and then we succeed by bounding from below the product of covolumes of those lattices. The proof of Theorem 4 is similar, but it focuses on successive minima in place of lattice point counts. In order to formulate the key arithmetic ingredient of both proofs, Theorem 5 below, we need to introduce further notation.

For a nonzero prime ideal $\mathfrak{p} \subset \mathfrak{o}$ dividing a rational prime p, let $e_\mathfrak{p}$ (resp. $f_\mathfrak{p}$) denote the ramification index (resp. inertia degree) of the local field extension $k_\mathfrak{p}/\mathbb{Q}_p$. By [13, Chapter III, Section 2], the exponent of $\mathfrak{p}$ in the different ideal of $\mathfrak{o}$ equals $e_\mathfrak{p} - 1$ when $p \nmid e_\mathfrak{p}$, and it lies between $e_\mathfrak{p}$ and $e_\mathfrak{p} - 1 + v_\mathfrak{p}(e_\mathfrak{p})$ when $p \mid e_\mathfrak{p}$ (which can only occur

for $p \leqslant d$). Therefore, the *tame discriminant* Δ_{tame}, defined as

$$\Delta_{\mathrm{tame}} := \prod_p p^{d-f_p} \quad \text{with} \quad f_p := \sum_{\mathfrak{p}|p} f_{\mathfrak{p}}, \tag{13}$$

divides the discriminant Δ, and it satisfies

$$|\Delta| < 2^{d^3} \Delta_{\mathrm{tame}}. \tag{14}$$

The last bound is rather crude, and it can be verified as follows. The ratio $\Delta/\Delta_{\mathrm{tame}}$ divides the norm of the ideal $\prod_{p\leqslant d}\prod_{\mathfrak{p}|p}\mathfrak{p}^{v_{\mathfrak{p}}(e_{\mathfrak{p}})}$, which is a divisor of the principal ideal $\prod_{p\leqslant d}\prod_{\mathfrak{p}|p}(e_{\mathfrak{p}})$. Therefore,

$$\frac{|\Delta|}{\Delta_{\mathrm{tame}}} \leqslant \prod_{p\leqslant d}\prod_{\mathfrak{p}|p} e_{\mathfrak{p}}^d < \prod_{p\leqslant d} 2^{d\sum_{\mathfrak{p}|p} e_{\mathfrak{p}}} < 2^{d^3}.$$

Theorem 5. Let $\mathfrak{n} \subset \mathfrak{o}$ be a nonzero ideal, and let $m \in \{1,\dots,d\}$. For any m-subsets $X \subset \mathfrak{n}$ and $S \subset \Sigma$,

$$\prod_{g\in G} \det{}^2(\sigma(x))_{x\in X}^{\sigma\in gS} \quad \text{is divisible by} \quad \Delta_{\mathrm{tame}}^{|G|\max\left(0,\frac{2m}{d}-1\right)}[\mathfrak{o}:\mathfrak{n}]^{|G|\frac{2m}{d}}. \tag{15}$$

If G is 2-homogeneous, then the exponent of Δ_{tame} can be improved to $|G|\frac{m(m-1)}{d(d-1)}$.

Note that d divides $|G|$, and also $\binom{d}{2}$ divides G when G is 2-homogeneous, so the exponents of Δ_{tame} and $[\mathfrak{o}:\mathfrak{n}]$ are nonnegative integers. The next theorem is very similar to the 2-homogeneous case of Theorem 5. We do not need it for the proof of Theorem 3, but we present it for its intrinsic beauty and interest.

Theorem 6. Let $\mathfrak{n} \subset \mathfrak{o}$ be a nonzero ideal, and let $m \in \{2,\dots,d\}$. For any m-subset $X \subset \mathfrak{n}$,

$$\prod_{\substack{S\subset\Sigma\\|S|=m}} \det{}^2(\sigma(x))_{x\in X}^{\sigma\in S} \quad \text{is divisible by} \quad \Delta_{\mathrm{tame}}^{\binom{d-2}{m-2}}[\mathfrak{o}:\mathfrak{n}]^{2\binom{d-1}{m-1}}. \tag{16}$$

The determinants in (15) and (16) are only defined up to a factor of ± 1 because we have not specified any ordering on X and S. However, their squares are well defined. If $m = d$, then Theorems 5 and 6 follow from the fact that either $\det(\sigma(x))_{x\in X}^{\sigma\in\Sigma}$ is zero or it equals the covolume of a full rank sublattice of $\mathfrak{n}$. Another relatively simple special

case is when $\mathfrak{n} = \mathfrak{o}$ and $X = \{1, x, \ldots, x^{m-1}\}$ for some $x \in \mathfrak{o}$. Then, Theorem 6 and the 2-homogeneous case of Theorem 5 are consequences of the Vandermonde determinant formula and the definition of the (usual) discriminant Δ of k. Not surprisingly, we shall only use the divisibility conclusion when the participating determinants are nonzero. On the other hand, it seems to be an interesting and difficult problem to characterize the vanishing of these determinants. One result in this direction is Chebotarev's theorem from 1926: if p is a prime, k is the p-th cyclotomic field, and the elements of X are p-th roots of unity, then none of these determinants vanish (see [16] for a proof and for useful references). Another result is the following simple observation: if k contains a proper subfield k' with $m = [k : k']$, and the m-subset $X \subset k$ is linearly dependent over k', then there is an m-subset $S \subset \Sigma$ such that all embeddings $\sigma \in S$ coincide on k', whence $\det(\sigma(x))_{x\in X}^{\sigma\in S} = 0$. Motivated by this example, we ask the following question:

Question. Assume that $X \subset k$ and $S \subset \Sigma$ satisfy $|X| = |S|$ and $\det(\sigma(x))_{x\in X}^{\sigma\in S} = 0$. Does there exist a subfield k' of k such that X is linearly dependent over k', and all embeddings $\sigma \in S$ coincide on k'?

If X is of size m and G is m-homogeneous (e.g., when $G = S_d$ or $G = A_d$), then the answer to this question is affirmative. Indeed, in this case, the vanishing of one $m \times m$ minor of $\det(\sigma(x))_{x\in X}^{\sigma\in\Sigma}$ implies the vanishing of all $m \times m$ minors, which can happen if and only if X is linearly dependent over $\mathbb{Q}$.

2 Non-Archimedean Investigations

In this section, we prove Theorems 5 and 6. The two sides of (15) and (16) are rational integers; hence, it suffices to show, for every rational prime p, that the exponent of p is at least as large on the left-hand side as on the right-hand side (with the convention that the p-exponent of zero is infinity).

We fix p and an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$, then we can think of the elements of Σ as the embeddings $\sigma : k \hookrightarrow \overline{\mathbb{Q}_p}$. For each $\sigma \in \Sigma$, there is a unique prime ideal $\mathfrak{p} \mid p$ and a unique $\mathbb{Q}_p$-linear extension $\tilde{\sigma} : k_\mathfrak{p} \hookrightarrow \overline{\mathbb{Q}_p}$ of σ. Denoting by $I_\mathfrak{p}$ the set of σs corresponding to a given $\mathfrak{p}$, the extension map $\sigma \mapsto \tilde{\sigma}$ is a bijection $I_\mathfrak{p} \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Q}_p}(k_\mathfrak{p}, \overline{\mathbb{Q}_p})$ with inverse being the restriction map. In particular, $I_\mathfrak{p}$ is a $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$-orbit on Σ of cardinality $[k_\mathfrak{p} : \mathbb{Q}_p] = e_\mathfrak{p} f_\mathfrak{p}$. Let v_p be the unique additive valuation on $\overline{\mathbb{Q}_p}$ extending the normalized additive valuation on $\mathbb{Q}_p$, and let $v_\mathfrak{p}$ be the normalized additive valuation on $k_\mathfrak{p}$. By "normalized" we mean that $v_p(\mathbb{Q}_p^\times) = \mathbb{Z}$ and $v_\mathfrak{p}(k_\mathfrak{p}^\times) = \mathbb{Z}$. Then, we have the important

identity

$$v_p(\tilde{\sigma}(x)) = \frac{1}{e_{\mathfrak{p}}} v_{\mathfrak{p}}(x), \qquad \tilde{\sigma} \in \mathrm{Hom}_{\mathbb{Q}_p}(k_{\mathfrak{p}}, \overline{\mathbb{Q}_p}), \qquad x \in k_{\mathfrak{p}}^{\times}. \tag{17}$$

See [13, Chapter II, Section 8] for more details. Let $l_{\mathfrak{p}}$ be the maximal unramified subextension of $k_{\mathfrak{p}}/\mathbb{Q}_p$, then

$$[k_{\mathfrak{p}} : l_{\mathfrak{p}}] = e_{\mathfrak{p}} \qquad \text{and} \qquad [l_{\mathfrak{p}} : \mathbb{Q}_p] = f_{\mathfrak{p}}.$$

Identifying $I_{\mathfrak{p}}$ with $\mathrm{Hom}_{\mathbb{Q}_p}(k_{\mathfrak{p}}, \overline{\mathbb{Q}_p})$ as above, we can break up $I_{\mathfrak{p}}$ into $f_{\mathfrak{p}}$ subsets $I_{\mathfrak{p},l}$ of equal size $e_{\mathfrak{p}}$ according to how $l_{\mathfrak{p}}$ gets embedded into $\overline{\mathbb{Q}_p}$. In the end, two elements of Σ belong to the same subset $I_{\mathfrak{p},l}$ if and only if they induce the same non-archimedean valuation $|\cdot|_{\mathfrak{p}}$ on k and their $\mathbb{Q}_p$-linear extensions agree on $l_{\mathfrak{p}}$; we shall call two such elements of Σ *inertially equivalent*.

The proofs of Theorems 5 and 6 rely on the key observation that the p-adic valuation of the participating determinants can be estimated in terms of the inertial equivalence classes $I_{\mathfrak{p},l}$.

Proposition 1. Let $\mathfrak{n} \subset \mathfrak{o}$ be a nonzero ideal, and let $m \in \{1, \dots, d\}$. For any m-subsets $X \subset \mathfrak{n}$ and $S \subset \Sigma$,

$$v_p\Big(\det{}^2(\sigma(x))_{x\in X}^{\sigma\in S}\Big) \geqslant \sum_{\mathfrak{p}\mid p} \frac{1}{e_{\mathfrak{p}}} \sum_{l=1}^{f_{\mathfrak{p}}} s_{\mathfrak{p},l}\big(2v_{\mathfrak{p}}(\mathfrak{n}) + s_{\mathfrak{p},l} - 1\big), \tag{18}$$

where $s_{\mathfrak{p},l}$ abbreviates $|S \cap I_{\mathfrak{p},l}|$, and $v_{\mathfrak{p}}(\mathfrak{n})$ stands for the exponent of $\mathfrak{p}$ in $\mathfrak{n}$.

Proof. We recall that K is the compositum of the fields $\sigma(k)$ for $\sigma \in \Sigma$, and we write $\tilde{K}$ for the extension of $\mathbb{Q}_p$ generated by K. We denote by $\tilde{d}$ the degree $[\tilde{K} : \mathbb{Q}_p]$, and by $\tilde{\mathfrak{o}}$ the ring of integers of $\tilde{K}$. We shall think of $\tilde{\mathfrak{o}}^m$ as the set of column vectors of length m with entries in $\tilde{\mathfrak{o}}$.

The m-set $S \subset \Sigma$ is partitioned into the $s_{\mathfrak{p},l}$-sets $S_{\mathfrak{p},l} := S \cap I_{\mathfrak{p},l}$. Accordingly, the $m \times m$ matrix $A := (\sigma(x))_{x\in X}^{\sigma\in S}$ decomposes into the $s_{\mathfrak{p},l} \times m$ blocks $A_{\mathfrak{p},l} := (\sigma(x))_{x\in X}^{\sigma\in S_{\mathfrak{p},l}}$. Strictly speaking, these matrices are only defined up to a permutation of the rows and the columns, but this ambiguity disappears once we choose an ordering of the rows and the columns.

We shall assume that $\det A \neq 0$, for otherwise (18) is trivial. The natural isomorphism from $\tilde{\mathfrak{o}}^m$ to $\prod_{\mathfrak{p}} \prod_l \tilde{\mathfrak{o}}^{s_{\mathfrak{p},l}}$ maps $A\tilde{\mathfrak{o}}^m$ into $\prod_{\mathfrak{p}} \prod_l A_{\mathfrak{p},l}\tilde{\mathfrak{o}}^m$; hence, it induces a

surjective homomorphism from $\tilde{\mathfrak{o}}^m/A\tilde{\mathfrak{o}}^m$ onto $\prod_{\mathfrak{p}}\prod_l(\tilde{\mathfrak{o}}^{s_{\mathfrak{p},l}}/A_{\mathfrak{p},l}\tilde{\mathfrak{o}}^m)$. In particular,

$$v_p\big([\tilde{\mathfrak{o}}^m : A\tilde{\mathfrak{o}}^m]\big) \geqslant \sum_{\mathfrak{p}\mid p}\sum_{l=1}^{f_{\mathfrak{p}}} v_p\big([\tilde{\mathfrak{o}}^{s_{\mathfrak{p},l}} : A_{\mathfrak{p},l}\tilde{\mathfrak{o}}^m]\big).$$

The left-hand side equals $\tilde{d}\cdot v_p(\det A)$, hence (18) will follow if we can show that

$$v_p\big([\tilde{\mathfrak{o}}^{s_{\mathfrak{p},l}} : A_{\mathfrak{p},l}\tilde{\mathfrak{o}}^m]\big) \geqslant \frac{\tilde{d}}{e_{\mathfrak{p}}}s_{\mathfrak{p},l}\left(v_{\mathfrak{p}}(\mathfrak{n}) + \frac{s_{\mathfrak{p},l}-1}{2}\right). \tag{19}$$

Let us fix $\mathfrak{p} \mid p$ and $l \in \{1,\dots,f_{\mathfrak{p}}\}$. We shall assume that $S_{\mathfrak{p},l}$ is not empty, for otherwise (19) is trivial. We write

$$t := s_{\mathfrak{p},l} \qquad \text{and} \qquad B := A_{\mathfrak{p},l} \tag{20}$$

to simplify notation, and we list the elements of $S_{\mathfrak{p},l}$ as $\{\sigma_1,\dots,\sigma_t\}$. By (17), we have

$$v_p(\tilde{\sigma}_i(x)) = \frac{1}{e_{\mathfrak{p}}}v_{\mathfrak{p}}(x), \qquad i \in \{1,\dots,t\}, \qquad x \in k_{\mathfrak{p}}^{\times}. \tag{21}$$

We also list the elements of X as $\{x_1,\dots,x_m\}$ in such a way that

$$v_{\mathfrak{p}}(\mathfrak{n}) \leqslant v_{\mathfrak{p}}(x_1) \leqslant \cdots \leqslant v_{\mathfrak{p}}(x_m).$$

In particular, v_p is constant on each column of

$$B = \begin{pmatrix} \sigma_1(x_1) & \cdots & \sigma_1(x_m) \\ \vdots & \ddots & \vdots \\ \sigma_t(x_1) & \cdots & \sigma_t(x_m) \end{pmatrix},$$

and it is non-decreasing from left to right. As the σ_is are inertially equivalent, their $\mathbb{Q}_p$-linear extensions $\tilde{\sigma}_i$ coincide on $l_{\mathfrak{p}}$, and we can identify $l_{\mathfrak{p}}$ with its image in $\tilde{K}$ via any of these embeddings. A nice feature resulting from this identification is that the $\tilde{\sigma}_i$s are $l_{\mathfrak{p}}$-linear, not just $\mathbb{Q}_p$-linear.

We are ready to prove (19). We shall use the fact that the left-hand side of (19), which is $[\tilde{\mathfrak{o}}^t : B\tilde{\mathfrak{o}}^m]$ in our new notation (20), remains unchanged if we multiply B by elements of $\mathrm{GL}_m(\tilde{\mathfrak{o}})$ on the right and by elements of $\mathrm{GL}_t(\tilde{\mathfrak{o}})$ on the left. Writing $\mathfrak{o}_{l_{\mathfrak{p}}}$ (resp. $\mathfrak{o}_{k_{\mathfrak{p}}}$) for the ring of integers of $l_{\mathfrak{p}}$ (resp. $k_{\mathfrak{p}}$), we shall also utilize the fact that the group

of units $\mathfrak{o}_{l_\mathfrak{p}}^\times$ contains a full set of representatives for the nonzero residue classes modulo $\mathfrak{p}\mathfrak{o}_{k_\mathfrak{p}}$ in $\mathfrak{o}_{k_\mathfrak{p}}$. This is because the residue fields of $l_\mathfrak{p}$ and $k_\mathfrak{p}$ have equal cardinality $p^{f_\mathfrak{p}}$.

First, we perform invertible elementary column operations over $\mathfrak{o}_{l_\mathfrak{p}}$ in order to increase the additive valuations of the columns of B. Specifically, we run the following algorithm:

(1) set $j = 1$;
(2) for each $j' \in \{j+1, \dots, m\}$, if $v_\mathfrak{p}(x_{j'}) = v_\mathfrak{p}(x_j)$, then choose $w \in \mathfrak{o}_{l_\mathfrak{p}}^\times$ such that $v_\mathfrak{p}(x_{j'} - wx_j) > v_\mathfrak{p}(x_j)$ and replace $x_{j'}$ by $x_{j'} - wx_j$;
(3) reorder $(x_{j+1}, \dots, x_m)$ in such a way that $v_\mathfrak{p}$ is non-decreasing on the new sequence;
(4) replace j by $j+1$;
(5) if $j < m$, then go to step (2); otherwise, finish.

We end up with a matrix

$$C = \begin{pmatrix} \tilde{\sigma}_1(y_1) & \cdots & \tilde{\sigma}_1(y_m) \\ \vdots & \ddots & \vdots \\ \tilde{\sigma}_t(y_1) & \cdots & \tilde{\sigma}_t(y_m) \end{pmatrix}$$

with $y_1, \dots, y_m \in \mathfrak{o}_{k_\mathfrak{p}}$ such that

$$v_\mathfrak{p}(\mathfrak{n}) \leqslant v_\mathfrak{p}(y_1) < \cdots < v_\mathfrak{p}(y_m).$$

In particular, $v_\mathfrak{p}(y_j) \geqslant v_\mathfrak{p}(\mathfrak{n}) + j - 1$ for all $j \in \{1, \dots, m\}$.

Second, we perform invertible elementary row operations over $\tilde{\mathfrak{o}}$ to transform C into

$$D = \begin{pmatrix} z_{1,1} & z_{1,2} & \cdots & z_{1,t} & \cdots & z_{1,m} \\ 0 & z_{2,2} & \cdots & z_{2,t} & \cdots & z_{2,m} \\ \vdots & \ddots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & z_{t,t} & \dots & z_{t,m} \end{pmatrix}$$

with $z_{i,j} \in \tilde{\mathfrak{o}}$ such that (cf. (21))

$$v_p(z_{i,j}) \geqslant \frac{1}{e_\mathfrak{p}}\big(v_\mathfrak{p}(\mathfrak{n}) + j - 1\big), \qquad i \leqslant j.$$

In particular, $D\tilde{\mathfrak{o}}^m$ is a subgroup of $\tilde{\mathfrak{n}}_1 \times \cdots \times \tilde{\mathfrak{n}}_t$, where

$$\tilde{\mathfrak{n}}_i := \left\{ z \in \tilde{\mathfrak{o}} : v_p(z) \geqslant \frac{1}{e_\mathfrak{p}}\big(v_\mathfrak{p}(\mathfrak{n}) + i - 1\big) \right\}, \qquad i \in \{1, \dots, t\}.$$

This implies, using that $e_{\mathfrak{p}}$ divides the ramification degree of the local field extension $\tilde{K}/\mathbb{Q}_p$,

$$v_p\big([\tilde{\mathfrak{o}}^t : D\tilde{\mathfrak{o}}^m]\big) \geqslant \sum_{i=1}^{t} v_p\big([\tilde{\mathfrak{o}} : \tilde{\mathfrak{n}}_i]\big) = \sum_{i=1}^{t} \frac{\tilde{d}}{e_{\mathfrak{p}}}\big(v_{\mathfrak{p}}(\mathfrak{n}) + i - 1\big). \tag{22}$$

The inequalities (22) and (19) are equivalent because their left-hand sides are equal and their right-hand sides are also equal (cf. (20)). The proof of Proposition 1 is complete. ■

Proof of Theorem 5. For any $g \in G$, it follows from Proposition 1 that

$$v_p\Big(\det{}^2(\sigma(x))_{x\in X}^{\sigma\in gS}\Big) \geqslant \sum_{\mathfrak{p}|p} \frac{1}{e_{\mathfrak{p}}} \sum_{l=1}^{f_{\mathfrak{p}}} \sum_{\sigma\in I_{\mathfrak{p},l}} 1_{gS}(\sigma) \left(2v_{\mathfrak{p}}(\mathfrak{n}) + \sum_{\sigma'\in I_{\mathfrak{p},l}\setminus\{\sigma\}} 1_{gS}(\sigma')\right).$$

We average both sides over $g \in G$, utilizing that G acts transitively and faithfully on Σ. For any $\sigma \in \Sigma$, we obtain readily that

$$\frac{1}{|G|}\sum_{g\in G} 1_{gS}(\sigma) = \frac{1}{|G|}\sum_{g\in G} 1_S(g^{-1}\sigma) = \frac{|S|}{d} = \frac{m}{d}. \tag{23}$$

As a consequence, for any distinct $\sigma, \sigma' \in \Sigma$, we see that

$$\frac{1}{|G|}\sum_{g\in G} 1_{gS}(\sigma)1_{gS}(\sigma') \geqslant \frac{1}{|G|}\sum_{g\in G}\big(1_{gS}(\sigma) + 1_{gS}(\sigma') - 1\big) = \frac{2m}{d} - 1. \tag{24}$$

This bound is trivial when $m < d/2$, in which case we shall only use that the left-hand side is nonnegative. Combining these inequalities and noting that $|I_{\mathfrak{p},l}| = e_{\mathfrak{p}}$, we infer that

$$\frac{1}{|G|}\sum_{g\in G} v_p\Big(\det{}^2(\sigma(x))_{x\in X}^{\sigma\in gS}\Big) \geqslant \sum_{\mathfrak{p}|p} f_{\mathfrak{p}}\left(v_{\mathfrak{p}}(\mathfrak{n})\frac{2m}{d} + (e_{\mathfrak{p}} - 1)\max\left(0, \frac{2m}{d} - 1\right)\right).$$

Now from $[\mathfrak{o} : \mathfrak{p}] = p^{f_{\mathfrak{p}}}$ it is clear that

$$\sum_{\mathfrak{p}|p} f_{\mathfrak{p}} v_{\mathfrak{p}}(\mathfrak{n}) = v_p\big([\mathfrak{o} : \mathfrak{n}]\big),$$

while (13) implies that

$$\sum_{\mathfrak{p}|p} f_{\mathfrak{p}}(e_{\mathfrak{p}}-1) = d - f_p = v_p(\Delta_{\mathrm{tame}}).$$

Therefore, the last inequality can be rewritten as

$$\frac{1}{|G|}\sum_{g\in G} v_p\left(\det{}^2(\sigma(x))_{x\in X}^{\sigma\in gS}\right) \geqslant \frac{2m}{d} v_p\left([\mathfrak{o}:\mathfrak{n}]\right) + \max\left(0, \frac{2m}{d}-1\right) v_p(\Delta_{\mathrm{tame}}).$$

The rational prime p was arbitrary here, so we have proved (15).

If G is 2-homogeneous, then we can improve (24) to

$$\frac{1}{|G|}\sum_{g\in G} 1_{gS}(\sigma)1_{gS}(\sigma') = \frac{1}{|G|}\sum_{g\in G} 1_S(g^{-1}\sigma)1_S(g^{-1}\sigma') = \frac{\binom{|S|}{2}}{\binom{d}{2}} = \frac{m(m-1)}{d(d-1)}.$$

As a result, we can replace $\max\left(0, \frac{2m}{d}-1\right)$ by $\frac{m(m-1)}{d(d-1)}$ in the subsequent argument, and hence also in (15). The proof of Theorem 5 is complete. ■

Proof of Theorem 6. For any m-subset $S \subset \Sigma$, it follows from Proposition 1 that

$$v_p\left(\det{}^2(\sigma(x))_{x\in X}^{\sigma\in S}\right) \geqslant \sum_{\mathfrak{p}|p}\frac{1}{e_{\mathfrak{p}}}\sum_{l=1}^{f_{\mathfrak{p}}}\sum_{\sigma\in I_{\mathfrak{p},l}} 1_S(\sigma)\left(2v_{\mathfrak{p}}(\mathfrak{n}) + \sum_{\sigma'\in I_{\mathfrak{p},l}\setminus\{\sigma\}} 1_S(\sigma')\right).$$

We sum both sides over all m-subsets $S \subset \Sigma$, using that

$$\sum_{\substack{S\subset\Sigma\\|S|=m}} 1_S(\sigma) = \binom{d-1}{m-1} \quad \text{for any } \sigma\in\Sigma;$$

$$\sum_{\substack{S\subset\Sigma\\|S|=m}} 1_S(\sigma)1_S(\sigma') = \binom{d-2}{m-2} \quad \text{for any distinct } \sigma,\sigma'\in\Sigma.$$

From here, we proceed as in the proof of Theorem 5 and conclude

$$\sum_{\substack{S\subset\Sigma\\|S|=m}} v_p\left(\det{}^2(\sigma(x))_{x\in X}^{\sigma\in S}\right) \geqslant 2\binom{d-1}{m-1} v_p\left([\mathfrak{o}:\mathfrak{n}]\right) + \binom{d-2}{m-2} v_p(\Delta_{\mathrm{tame}}).$$

The rational prime p was arbitrary here, so the proof of Theorem 6 is complete. ■

3 Archimedean Investigations

In this section, we prove Theorems 3–4 and Corollaries 1–4. We shall combine Theorems 1 and 5 with the following lesser known result of Blichfeldt [2], of which Theorem 2 is a special case.

Theorem 7 (Blichfeldt [2]). Let $\Lambda \subset \mathbb{R}^m$ be a lattice, and let $\mathcal{C} \subset \mathbb{R}^m$ be a convex body containing the origin. If $\Lambda \cap \mathcal{C}$ contains m linearly independent lattice vectors, then

$$|\Lambda \cap \mathcal{C}| \leqslant m! \frac{\mathrm{vol}(\mathcal{C})}{\det(\Lambda)} + m \leqslant (m+1)! \frac{\mathrm{vol}(\mathcal{C})}{\det(\Lambda)}. \tag{25}$$

Proof. The second inequality is clear by $\mathrm{vol}(\mathcal{C}) \geqslant \det(\Lambda)/m!$; hence, we focus on the first inequality. In this proof, a polytope (resp. simplex) will always mean a convex lattice polytope (resp. simplex) with vertices lying in Λ. For other terminology, we follow the book [5]. By the initial assumptions on $\mathcal{C}$, the convex hull of $\Lambda \cap \mathcal{C}$ is an m-dimensional polytope, which can be decomposed into m-simplices according to [5, Proposition 2.2.4]. The corresponding triangulation of $\Lambda \cap \mathcal{C}$ can be refined to a full triangulation by decomposing recursively the participating m-simplices into smaller m-simplices. Alternatively, one can obtain a full triangulation of $\Lambda \cap \mathcal{C}$ by ordering its elements in such a way that no point belongs to the convex hull of previous points, and then taking the placing/pushing triangulation for that ordering. We fix a full triangulation of $\Lambda \cap \mathcal{C}$, and we denote by $\mathcal{T}$ the set of m-simplices that participate in it. We define a graph on $\mathcal{T}$ by declaring that two elements of $\mathcal{T}$ are connected by an edge if and only if their intersection is an $(m-1)$-simplex. One can show that this graph is connected, which forces

$$|\mathcal{T}| \geqslant |\Lambda \cap \mathcal{C}| - m.$$

For details, see [5, Theorem 2.6.1], [14, Theorem 3.2] and their proofs. On the other hand, as $\mathcal{C}$ is convex and each element of $\mathcal{T}$ has volume at least $\det(\Lambda)/m!$, we also have

$$\mathrm{vol}(\mathcal{C}) \geqslant \mathrm{vol}(\cup \mathcal{T}) \geqslant \frac{\det(\Lambda)}{m!} |\mathcal{T}|.$$

Combining these two bounds, we get the first inequality of (25). As remarked earlier, the second inequality of (25) is straightforward, so the proof of Theorem 7 is complete. ■

Proof of Theorem 3. If $m = 0$, then (3) and (4) are trivial, so we shall assume that $0 < m < d$. We write V for the $\mathbb{R}$-span of $\mathfrak{n} \cap \mathcal{B}$, so that V is an m-dimensional $\mathbb{R}$-subspace of $k \otimes_{\mathbb{Q}} \mathbb{R}$, and $\mathfrak{n} \cap V$ is an m-dimensional lattice in V. We fix a basis $X \subset \mathfrak{n}$

of $\mathfrak{n} \cap V$, and we think of its elements as the columns of the $d \times m$ complex matrix $M := (\sigma(x))_{x\in X}^{\sigma\in\Sigma}$. Strictly speaking, M is only defined up to a permutation of the rows and the columns, but this ambiguity disappears once we choose an ordering of Σ and X. By construction, the columns of M are linearly independent over $\mathbb{R}$, and we claim that they are also linearly independent over $\mathbb{C}$. Indeed, if $c : X \to \mathbb{C}$ satisfies $\sum_{x\in X} c(x)\sigma(x) = 0$ for all $\sigma \in \Sigma$, then complex conjugating the equations and switching from σ to $\overline{\sigma}$, we get that $\sum_{x\in X} \overline{c(x)}\sigma(x) = 0$ for all $\sigma \in \Sigma$. As a result, the real and imaginary parts of $c(x)$ must vanish for all $x \in X$, which proves the claim. Hence, $\operatorname{rank}(M) = m$, and there exists an m-subset $S \subset \Sigma$ such that $\det(\sigma(x))_{x\in X}^{\sigma\in S} \neq 0$. We fix $S \subset \Sigma$ along with $X \subset \mathfrak{n}$.

For any Galois automorphism $g \in G$, the image of $\det(\sigma(x))_{x\in X}^{\sigma\in S}$ under g equals $\det(\sigma(x))_{x\in X}^{\sigma\in gS}$. Therefore, these $m \times m$ minors of M are nonzero, and by (14) and Theorem 5 they satisfy

$$\prod_{g\in G} \left|\det(\sigma(x))_{x\in X}^{\sigma\in gS}\right| \gg_d |\Delta|^{|G|\max\left(0,\frac{m}{d}-\frac{1}{2}\right)}[\mathfrak{o} : \mathfrak{n}]^{|G|\frac{m}{d}}. \tag{26}$$

Moreover, the exponent of $|\Delta|$ can be improved to $|G|\frac{m(m-1)}{2d(d-1)}$ when G is 2-homogeneous.

Fixing $g \in G$ for a moment, the multilinearity of the determinant shows that there is a choice of $\tilde{\sigma} \in \{\operatorname{Re}(\sigma), \operatorname{Im}(\sigma)\}$ for each $\sigma \in gS$ such that

$$\left|\det(\sigma(x))_{x\in X}^{\sigma\in gS}\right| \leqslant 2^m \left|\det(\tilde{\sigma}(x))_{x\in X}^{\sigma\in gS}\right|. \tag{27}$$

The left-hand side is positive; hence, the right-hand side is also positive. Let $f : \mathbb{C}^\Sigma \to \mathbb{R}^{gS}$ be the product of the $\mathbb{R}$-linear surjections $f_\sigma : \mathbb{C} \to \mathbb{R}$ given by

$$f_\sigma(z) := \begin{cases} \operatorname{Re}(z), & \sigma \in gS \text{ and } \tilde{\sigma} = \operatorname{Re}(\sigma); \\ \operatorname{Im}(z), & \sigma \in gS \text{ and } \tilde{\sigma} = \operatorname{Im}(\sigma); \\ 0, & \sigma \notin gS. \end{cases}$$

Tautologically, $\tilde{\sigma} = f_\sigma \circ \sigma$ holds for all $\sigma \in gS$; hence, f restricts to an $\mathbb{R}$-linear isomorphism $V \xrightarrow{\sim} \mathbb{R}^{gS}$, and $\Lambda := f(\mathfrak{n} \cap V)$ is a lattice in $\mathbb{R}^{gS}$ of covolume $\left|\det(\tilde{\sigma}(x))_{x\in X}^{\sigma\in gS}\right|$. In addition, $\mathcal{C} := f(\mathcal{B})$ is an o-symmetric convex body in $\mathbb{R}^{gS}$, which lies in the orthotope $\prod_{\sigma\in gS}[-B_\sigma, B_\sigma]$ by (1). Clearly, $\Lambda \cap \mathcal{C}$ contains $f(\mathfrak{n} \cap \mathcal{B})$, which in turn contains m linearly independent lattice vectors. Now, we combine these observations with Theorem 7 and (27) to infer that

$$|\mathfrak{n} \cap \mathcal{B}| \leqslant |\Lambda \cap \mathcal{C}| \leqslant 4^m(m+1)! \frac{\prod_{\sigma\in gS} B_\sigma}{\left|\det(\sigma(x))_{x\in X}^{\sigma\in gS}\right|}.$$

We keep the two sides of the last inequality and take their geometric mean over $g \in G$. Using also (2), (23), and (26), we obtain

$$|\mathfrak{n} \cap \mathcal{B}| \ll_d \frac{\mathrm{vol}(\mathcal{B})^{\frac{m}{d}}}{|\Delta|^{\max\left(0, \frac{m}{d}-\frac{1}{2}\right)}[\mathfrak{o} : \mathfrak{n}]^{\frac{m}{d}}}. \tag{28}$$

Finally, we invoke Theorem 1 to estimate from above the right-hand side in terms of the left-hand side:

$$|\mathfrak{n} \cap \mathcal{B}| \ll_d |\mathfrak{n} \cap \mathcal{B}|^{\frac{m}{d}} |\Delta|^{\min\left(\frac{m}{2d}, \frac{1}{2}-\frac{m}{2d}\right)}. \tag{29}$$

This bound is equivalent to (3) in the light of $0 < m < d$. If G is 2-homogeneous, then the exponent of $|\Delta|$ can be improved to $\frac{m(m-1)}{2d(d-1)}$ in (28), and to $\frac{m(d-m)}{2d(d-1)}$ in (29), so that the resulting bound is equivalent to (4). The proof of Theorem 3 is complete. ■

Proof of Corollary 1. If $\mathfrak{n} \cap \mathcal{B}$ contains d linearly independent vectors, then (5) follows from Theorem 2. If $\mathfrak{n} \cap \mathcal{B}$ does not contain d linearly independent vectors, then (5) follows from Theorem 3. The proof of Corollary 1 is complete. ■

Proof of Corollary 2. In the light of Theorem 1, the bound (6) follows from (3), while the bound (7) follows from (4). The proof of Corollary 2 is complete. ■

Proof of Corollary 3. Assume that $\mathcal{B}$ does not contain a lattice basis of $\mathfrak{n}$. Then, by an observation of Mahler [10] (see also [6, Chapter 2, Section 10.2]), the scaled body $\frac{1}{d}\mathcal{B}$ does not contain d linearly independent lattice vectors from $\mathfrak{n}$. Hence, by Corollary 2, it follows that

$$\mathrm{vol}(\mathcal{B}) \ll_d \mathrm{vol}(\tfrac{1}{d}\mathcal{B}) \ll_d |\Delta|[\mathfrak{o} : \mathfrak{n}].$$

The proof of Corollary 3 is complete. ■

Proof of Theorem 4. We borrow several ideas from the proof of Theorem 3 without further mention. Let $x_1, \dots, x_m \in \mathfrak{n}$ be linearly independent lattice vectors whose Euclidean norms in $k \otimes_{\mathbb{Q}} \mathbb{R}$ are the successive minima $\lambda_1, \dots, \lambda_m$, respectively. Let X be the m-set $\{x_1, \dots, x_m\} \subset \mathfrak{n}$, and let V be the $\mathbb{R}$-span of X. Then, V is an m-dimensional $\mathbb{R}$-subspace of $k \otimes_{\mathbb{Q}} \mathbb{R}$, and $\mathfrak{n} \cap V$ is an m-dimensional lattice in V of successive minima $\lambda_1 \leqslant \cdots \leqslant \lambda_m$. In particular, the covolume of $\mathfrak{n} \cap V$ is $\asymp_d \lambda_1 \cdots \lambda_m$. We fix an m-subset $S \subset \Sigma$ such that $\det(\sigma(x))_{x \in X}^{\sigma \in S} \neq 0$. For any $g \in G$, there exists an orthogonal projection f of $k \otimes_{\mathbb{Q}} \mathbb{R}$ onto an m-subspace such that the covolume of $f(\mathfrak{n} \cap V)$ is at least

$2^{-m}\left|\det(\sigma(x))_{x\in X}^{\sigma\in gS}\right|$. Since the covolume of $f(\mathfrak{n}\cap V)$ cannot exceed the covolume of $\mathfrak{n}\cap V$, we infer that

$$\lambda_1\cdots\lambda_m \gg_d \left|\det(\sigma(x))_{x\in X}^{\sigma\in gS}\right|, \qquad g\in G.$$

Taking the geometric mean of both sides over $g\in G$, and using (26), we obtain (8). Taking the reciprocal of (8), and then multiplying both sides by (12), we arrive at (9). If G is 2-homogeneous, then the exponent of $|\Delta|$ in (26) can be improved to $|G|\frac{m(m-1)}{2d(d-1)}$, and our argument yields the following variants of (8) and (9):

$$\lambda_1\cdots\lambda_m \gg_d |\Delta|^{\frac{m(m-1)}{2d(d-1)}}[\mathfrak{o}:\mathfrak{n}]^{\frac{m}{d}}; \tag{30}$$

$$\lambda_{m+1}\lambda_{m+2}\cdots\lambda_d \ll_d |\Delta|^{\frac{(d-m)(d+m-1)}{2d(d-1)}}[\mathfrak{o}:\mathfrak{n}]^{1-\frac{m}{d}}. \tag{31}$$

The proof of Theorem 4 is complete. ■

Proof of Corollary 4. We observe that (8) and (30) are also valid for $m=d$, while (9) and (31) are also valid for $m=0$. Indeed, these special cases amount to (12). Now, taking the m-th root of (8) and (30) readily yields the lower bound of (10) and (11). Similarly, taking the $(d-m)$-th root of (9) and (31) readily yields the upper bound of (10) and (11) with $m+1$ in place of m. The proof of Corollary 4 is complete. ■

4 Connections to the Work of McMullen [11] and Bhargava *et al.* [1]

If the number field k is totally real, then we can identify the $\mathbb{R}$-algebra $k\otimes_{\mathbb{Q}}\mathbb{R}$ with the set of column vectors $(z_\sigma)\in\mathbb{R}^\Sigma$. The multiplicative group $(\mathbb{R}^\Sigma)^\times$ acts on $\mathbb{R}^\Sigma$ by multiplication; hence, so does its subgroup

$$A := \left\{(a_\sigma)\in(0,\infty)^\Sigma : \prod_{\sigma\in\Sigma} a_\sigma = 1\right\}.$$

Let us consider the induced action of A on the space of lattices of $\mathbb{R}^\Sigma$. Geometrically, the space of lattices can be described as $\mathrm{GL}(\mathbb{R}^\Sigma)/\mathrm{GL}(\mathbb{Z}^\Sigma)$, and the induced action of A is given by left multiplication by positive diagonal matrices of determinant 1. In particular, this action is continuous and preserves the covolume. The group of totally positive units $\mathfrak{o}_+^\times$ is cocompact in A (cf. Dirichlet's unit theorem) and stabilizes the lattice $\mathfrak{o}$; hence, the orbit $A\mathfrak{o}$ is compact. By a striking result of McMullen [11, Theorem 4.1], the compactness of $A\mathfrak{o}$ implies the existence of $a\in A$ such that the successive minima of the lattice $a\mathfrak{o}$ are equal: $\mu_1=\cdots=\mu_d$. As we shall explain in the next paragraph, this fact gives rise to a short alternative proof of Corollary 3 (when k is totally real). We note in passing

that Levin *et al.* [9, Theorem 1.1] have extended McMullen's theorem to closed orbits of lattices; these orbits arise from direct sums of totally real number fields and their full rank additive subgroups [15, Proposition 5.7].

Let μ be the common value of $\mu_1 = \cdots = \mu_d$, and let $\mathcal{D}$ be the closed Euclidean unit ball in $\mathbb{R}^\Sigma$ centered at the origin. Then, $a\mathfrak{o} \cap \mu\mathcal{D}$ contains d linearly independent vectors. Let $\mathfrak{n} \subset \mathfrak{o}$ be a nonzero ideal, and let $\mathcal{B} \subset \mathbb{R}^\Sigma$ be an orthotope of the form $\prod_{\sigma\in\Sigma}[-B_\sigma, B_\sigma]$. We claim that if $\mathcal{B}$ does not contain a lattice basis of $\mathfrak{n}$, then

$$\mathrm{vol}(\mathcal{B}) \leqslant (2d\mu)^d |\Delta|^{1/2}[\mathfrak{o} : \mathfrak{n}]. \tag{32}$$

This is sufficient for the conclusion of Corollary 3, since $\mu^d = \mu_1 \cdots \mu_d \asymp_d |\Delta|^{1/2}$. Let us assume that (32) is false. Then, $\mathrm{vol}(a\mu^{-1}d^{-1}\mathcal{B}) > 2^d|\Delta|^{1/2}[\mathfrak{o} : \mathfrak{n}]$; hence, Theorem 1 guarantees the existence of a nonzero lattice point $x \in \mathfrak{n} \cap a\mu^{-1}d^{-1}\mathcal{B}$. By our initial remarks, $x\mathfrak{o} \cap xa^{-1}\mu\mathcal{D}$ contains d linearly independent vectors, so by $\mathfrak{n}\mathfrak{o} \subset \mathfrak{n}$ and $\mathcal{B}\mathcal{D} \subset \mathcal{B}$ it follows that $\mathfrak{n} \cap d^{-1}\mathcal{B}$ also contains d linearly independent vectors. Finally, by the earlier quoted observation of Mahler [10] (see also [6, Chapter 2, Section 10.2]), we conclude that $\mathcal{B}$ contains a lattice basis of $\mathfrak{n}$.

Corollary 3 can also be connected to the work of Bhargava *et al.* [1] in multiple ways. Let k be an arbitrary number field, and let $\lambda_1 \leqslant \cdots \leqslant \lambda_d$ be the successive minima of $\mathfrak{o}$ embedded as a lattice in $k \otimes_{\mathbb{Q}} \mathbb{R}$. Then, [1, Theorem 1.6] states that

$$\lambda_d \ll_d |\Delta|^{1/d}. \tag{33}$$

We claim that (33) follows from Corollary 3, while a weaker version of Corollary 3 follows from (33). To justify the first claim, we set $B_\sigma := \frac{1}{d+1}\lambda_d$ for all $\sigma \in \Sigma$ in (1). Clearly, $\mathcal{B}$ contains no lattice basis of $\mathfrak{o}$; hence, $\mathrm{vol}(\mathcal{B}) \ll_d |\Delta|$ by Corollary 3, which is equivalent to (33) by (2). To justify the second claim, we start from (33). Let $\mathfrak{n} \subset \mathfrak{o}$ be a nonzero ideal, and let $\mathcal{B} \subset k \otimes_{\mathbb{Q}} \mathbb{R}$ be a convex body of the form (1) not containing a lattice basis of $\mathfrak{n}$. As $\mathfrak{o} \cap \lambda_d\mathcal{D}$ contains d linearly independent vectors, we can proceed as in the previous paragraph but with $a \in A$ (resp. μ) replaced by $1 \in k$ (resp. λ_d). We deduce the following variant of (32):

$$\mathrm{vol}(\mathcal{B}) \leqslant (2d\lambda_d)^d |\Delta|^{1/2}[\mathfrak{o} : \mathfrak{n}] \ll_d |\Delta|^{3/2}[\mathfrak{o} : \mathfrak{n}].$$

That is, (33) alone implies a version of Corollary 3 in which $|\Delta|$ is replaced by $|\Delta|^{3/2}$.

Acknowledgments

We are grateful to the referees for their careful reading and valuable comments. We also thank Péter Pál Pálfy and Gergely Zábrádi for helpful discussions.

Funding

This research was supported by European Research Council grant CoG 648017 (M.F. & G.H.), the MTA Rényi Intézet Lendület Automorphic Research Group (G.H. & P.M.), National Research, Development and Innovation Office grant K 119528 (G.H. & P.M.), and the Premium Postdoctoral Fellowship of the Hungarian Academy of Sciences (P.M.)

References

[1] Bhargava, M., A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y. Zhao. "Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves." *J. Amer. Math. Soc.* To appear, arXiv:1701.02458.

[2] Blichfeldt, H. F. "Notes on geometry of numbers. The October meeting of the San Francisco section." *Bull. Amer. Math. Soc.* 27 (1921): 149–53.

[3] Cameron, P. J. "Finite permutation groups and finite simple groups." *Bull. London Math. Soc.* 13 (1981): 1–22.

[4] van der Corput, J. G. "Verallgemeinerung einer Mordellschen Beweismethode in der Geometrie der Zahlen." *Acta Arith.* 1 (1935): 62–6. Zweite Mitteilung, ibid. 2 (1936): 145–6.

[5] De Loera, J. A., J. Rambau, and F. Santos. Triangulations: Structures for Algorithms and Applications. *Algorithms and Computation in Mathematics*, Vol. 25. Berlin: Springer, 2010.

[6] Gruber, P. M. and C. G. Lekkerkerker. Geometry of Numbers. *North–Holland Mathematical Library*, Vol. 37, 2nd ed. Amsterdam: North–Holland Publishing Co., 1987.

[7] Huber, M. "The classification of flag-transitive Steiner 3-designs." *Adv. Geom.* 5 (2005): 195–221.

[8] Kantor, W. M. "Automorphism groups of designs." *Math. Z.* 109 (1969): 246–52.

[9] Levin, M., U. Shapira, and B. Weiss. "Closed orbits for the diagonal group and well-rounded lattices." *Groups Geom. Dyn.* 10 (2016): 1211–25.

[10] Mahler, K. "A theorem on inhomogeneous diophantine inequalities." *Proc. Kon. Ned. Akad. Wet.* 41 (1938): 634–7.

[11] McMullen, C. T. "Minkowski's conjecture, well-rounded lattices and topological dimension." *J. Amer. Math. Soc.* 18 (2005): 711–34.

[12] Minkowski, H. "Über die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen." *J. Reine Angew. Math.* 107 (1891): 278–97.

[13] Neukirch, J. Algebraische Zahlentheorie. Berlin: Springer, 1992.

[14] Rothschild, B. L. and E. G. Straus. "On triangulations of the convex hull of n points." *Combinatorica* 5 (1985): 167–79.

[15] Shapira, U. and B. Weiss. "On the Mordell–Gruber spectrum." *Int. Math. Res. Not. IMRN* 2015, no. 14 (2015): 5518–59.

[16] Tao, T. "An uncertainty principle for cyclic groups of prime order." *Math. Res. Lett.* 12 (2005): 121–7.